user is obtained. The reconstructed signed response string is verified using the server-side cryptographic function. A card reader reads the security device. The signed response string is encoded. The signed response string is decoded. The challenge string is forwarded to the dial-up client. The challenge string is forwarded to the PKI-Bridge. Packets are forwarded from the custom script dynamically linked library.

[0024] In general, in one aspect, the invention comprises an apparatus of integrating via a dial-up interface. The invention comprises means for sending session initiation information from a dial-up client to a PKI-Bridge, means for checking session initiation information by the PKI-Bridge, means for generating a challenge string by a server-side cryptographic function, means for forwarding the challenge string to a custom script dynamically linked library, means for forwarding the challenge string to a client-side cryptographic function from the custom script dynamically linked library, means for retrieving a private key from a security device, means for generating a response string, means for signing the response string with the private key of a dial-in user, means for forwarding a signed response string to the custom script dynamically linked library, means for dividing the signed response string into packets, means for forwarding packets to the PKI-Bridge, means for reconstructing the signed response string from packets, means for forwarding a reconstructed signed response string to the server-side cryptographic function, means for obtaining a public key of the dial-in user, and means for verifying the reconstructed signed response string using the server-side cryptographic function.

[0025] Other aspects and advantages of the invention will be apparent from the following description and the appended claims.

Brief Description of Drawings

[0026] Figure 1 illustrates a typical network workgroup.

[0027] Figure 2 illustrates a typical computer system.

[0028] Figure 3 illustrates a block diagram of a system in accordance with an embodiment of the present invention.

[0029] Figure 4 illustrates a user interface for a phone number and modem setup dialog box, in accordance with one or more embodiments of the present invention.

[0030] Figure 5 illustrates a user interface for a connection information dialog box, in accordance with one or more embodiments of the present invention.

[0031] Figure 6 illustrates a password input dialog box, in accordance with one or more embodiments of the present invention.

[0032] Figure 7 illustrates an error dialog box, in accordance with one or more embodiments of the present invention.

[0033] Figure 8 illustrates a flow chart describing a process, in accordance with one or more embodiments of the present invention.

[0034] Figure 9 illustrates a flow chart describing a process, in accordance with one or more embodiments of the present invention.

Detailed Description

[0035] Specific embodiments of the invention will now be described in detail with reference to the accompanying figures. Like elements in the various figures are denoted by like reference numerals for consistency.

[0036] In the following detailed description of the invention, numerous specific details are set forth in order to provide a more thorough understanding of the invention. However, it will be apparent to one of ordinary skill in the art that the invention may be practiced without these specific details. In other instances, well-known features have not been described in detail to avoid obscuring the invention.

[0037] The invention described herein may involve any computer regardless of the platform being used. For example, as shown in Figure 2, a typical computer (40) has a processor (42), memory (44), and numerous other elements and functionalities typical to today's computers (not shown). The computer (40) has associated therewith input means such as a keyboard (46), a mouse (48), and a card reader (50), although in an accessible environment these input means may take other forms. The computer (40) is also associated with an output device such as a display (52), which may also take a different form in an accessible environment. Finally, the computer (40) is connected to a wide area network (32), such as the Internet.

[0038] In one or more embodiments, the present invention involves a network system described herein as SmartDial. SmartDial is a Remote Access Server (RAS)-Public Key Infrastructure (PKI) product that integrates security devices, (*e.g.*, smart cards), a PKI encryption system (*e.g.*, Entrust), and a server (*e.g.*, RADIUS) via a dial-up interface. Referring to Figure 3, SmartDial involves the integration of numerous components including a client computer (102), a card reader (50) with reader firmware (105), a security device (106) (*e.g.*, a smart card) with an embedded CPU (107), a PC modem (108) individually or as part of a modem pool (not shown), a Network Access Point (NAP), *e.g.*, Remote Access Switch (110) with an Access Control and a RADIUS Proxy library (109), a server (112), *e.g.*, a RADIUS server, and a Directory Service (113), *e.g.*, a LDAP-compliant directory, located on a directory server (114).

[0039] For successful integration of all components, a plurality of custom modules and programming interfaces are required. Referring to Figure 3, a first custom module is a dial-up client (120), which is an executable program. A second